WEBINAR: IHR ACCOUNT IN FREMDEN HÄNDEN? EINBLICKE AUS UNSEREM SOC

first frame networkers

HERZLICH WILLKOMMEN

first frame networkers

Vielen Dank, dass Sie sich die Zeit für uns nehmen!

Was Sie heute erwartet:

Wie wir Account-Übernahmen im SOC live entlarven und Ihre Identitäten mit gezielten Strategien vor modernen Angriffen schützen.

Das Webinar wird in Schweizerdeutsch gehalten.

JÖRG KOCH
Leiter Marketing
first frame networkers ag

HERZLICH WILLKOMMEN

first frame networkers

PHILIPPE HIRZEL

Projektleiter Security Services
first frame networkers ag

- Seit insgesamt 8 Jahren bei der first frame networkers ag.
- Seine Aufgabe: Managed Services im Security-Bereich auf- und auszubauen.
- Aktuell studiert er am SANS Technology Institute für den Master of Science in Information Security Engineering.
- Neben der Arbeit kocht Philippe Hirzel gerne und ist Jugend- und Sport-Leiter (Ski).

HERZLICH WILLKOMMEN

first frame networkers

ARVEENAN KAMALAKUMARAN
Systems Engineer
first frame networkers ag

Heutiger Co-Referent:

- Seine Aufgabe: Systems Engineer und SOC-Agent
- Nach seiner kaufmännischen Ausbildung schloss er ein Informatikstudium (HF) mit Schwerpunkt Systemtechnik ab.
- Neben der Arbeit verbringt Arveenan gerne Zeit mit Freunden beim Sport oder einem gemütlichen Abend bei einer spannenden Serie oder einem guten Film.

AGENDA

first frame networkers

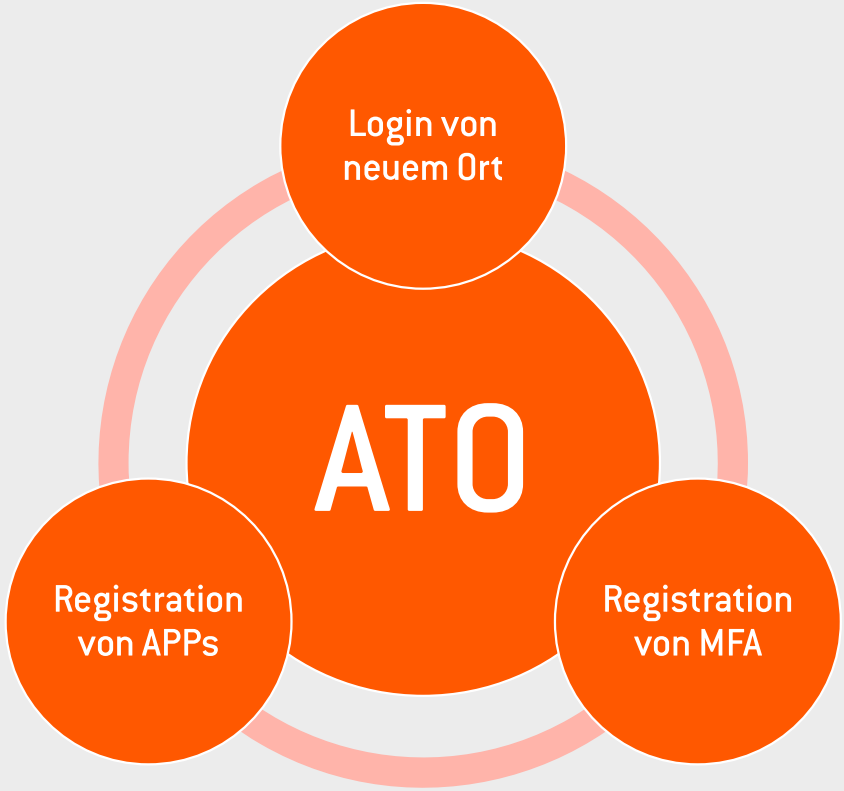
- 11:00 Begrüssung
- 11:05 Account Takeover - Wie hilft ein SOC & Praxisbeispiele
- 11:35 Fragen & Antworten
- 11:45 Schluss

Fragen können mit der Chatfunktion gestellt werden.

WAS IST ACCOUNT TAKE OVER?

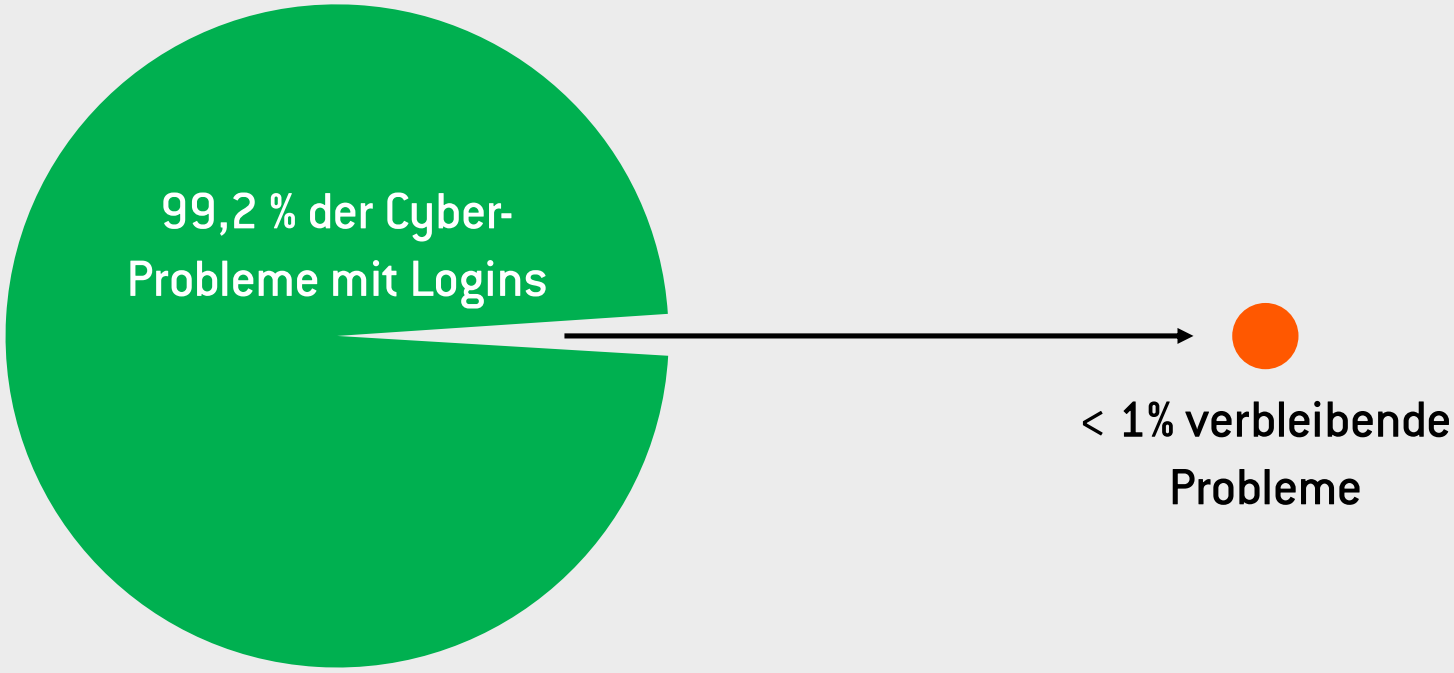
first frame networkers

- Übernahme eines Benutzerkontos
  - Versand von SPAM
  - Allgemeiner Betrug
  - Business E-Mail Compromise
  - Daten stehlen



MFA IST ESSENZIELL

first frame networkers



Microsoft Digital Defense Report 2024

MFA-BEISPIEL

first frame networkers

philippe.hirzel@firstframe.net

Approve sign in request

Open your Authenticator app, and enter the number shown to sign in.

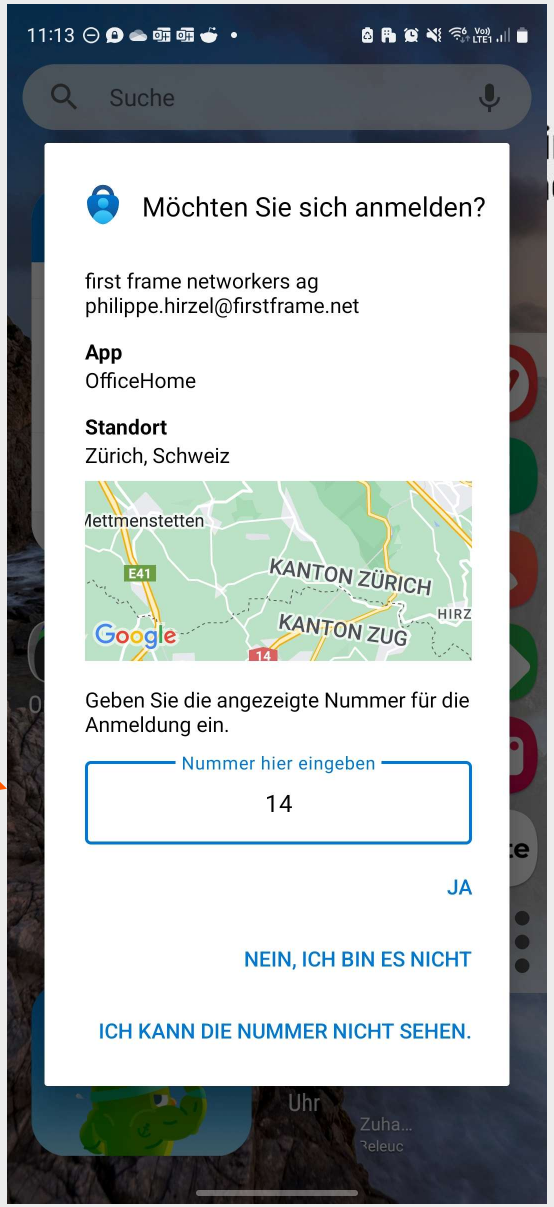
14

No numbers in your app? Make sure to upgrade to the latest version.

I can't use my Microsoft Authenticator app right now

More information

Für Unterstützung Bitte den Service Desk anrufen
+41 41 768 08 88



Microsoft Digital Defense Report 2024

FAKTOREN FÜR AUTHENTIFIZIERUNG

first frame networkers

- Etwas das man weiss
- Z.B. ein Passwort
- Kann verraten werden

- LinkedIn Passwörter wurden gestohlen
- Mark Zuckerberg hatte das Passwort «dadada»
- Auch auf Twitter & Pinterest

- Etwas das man hat
- Z.B. ein Smartphone
- Kann gestohlen werden

- Etwas das man ist
- Z.B. ein Fingerabdruck
- Kann gefälscht werden

MFA – MULTI FAKTOR AUTHENTIFIZIERUNG

first frame networkers

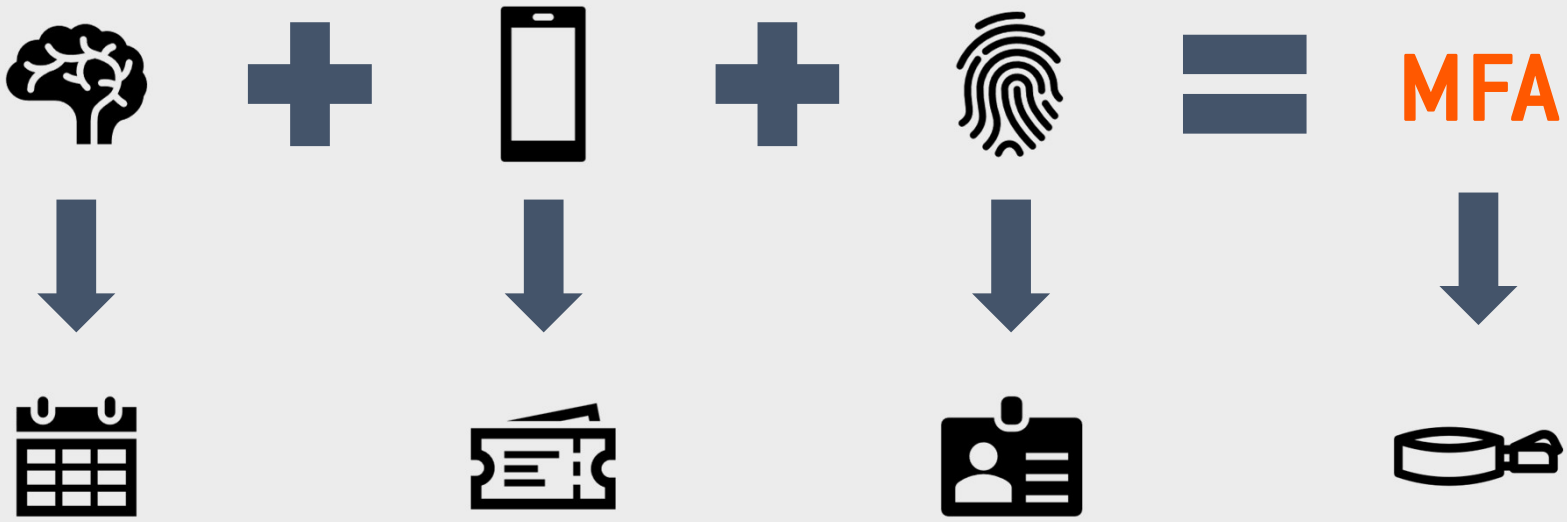
WIESO KANN EIN ACCOUNT ÜBERNOMMEN WERDEN?

WIESO KANN EIN ACCOUNT ÜBERNOMMEN WERDEN?

first frame networkers

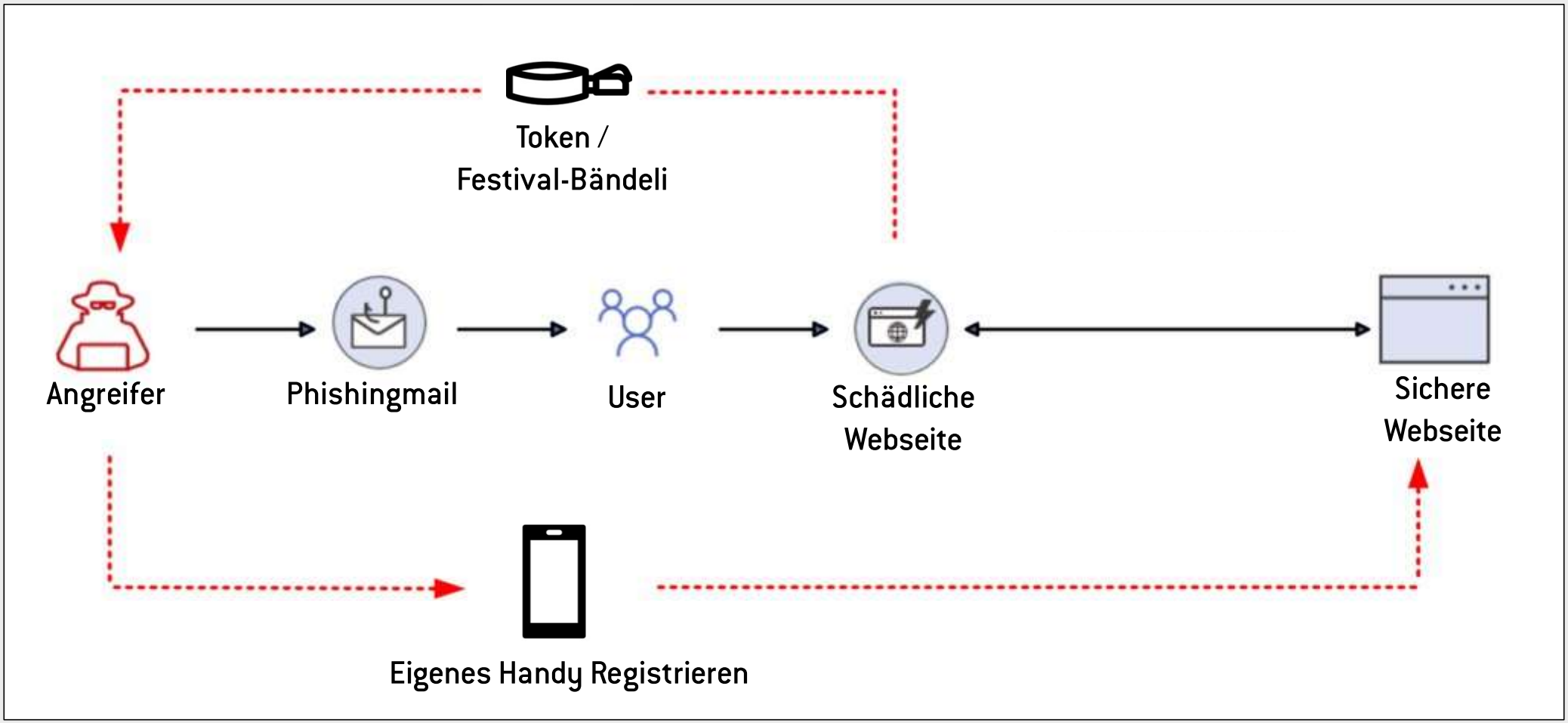
WIESO KANN EIN ACCOUNT ÜBERNOMMEN WERDEN?

first frame networkers



WIESO KANN EIN ACCOUNT ÜBERNOMMEN WERDEN?

first frame networkers



WIESO SPRECHEN WIR ÜBER ATO

first frame networkers

Vorfälle

- Kunden jeder Grösse
- Mind. jeden zweiten Monat
- Tendenz zunehmend
- 3 Vorfälle im Jahr 2026

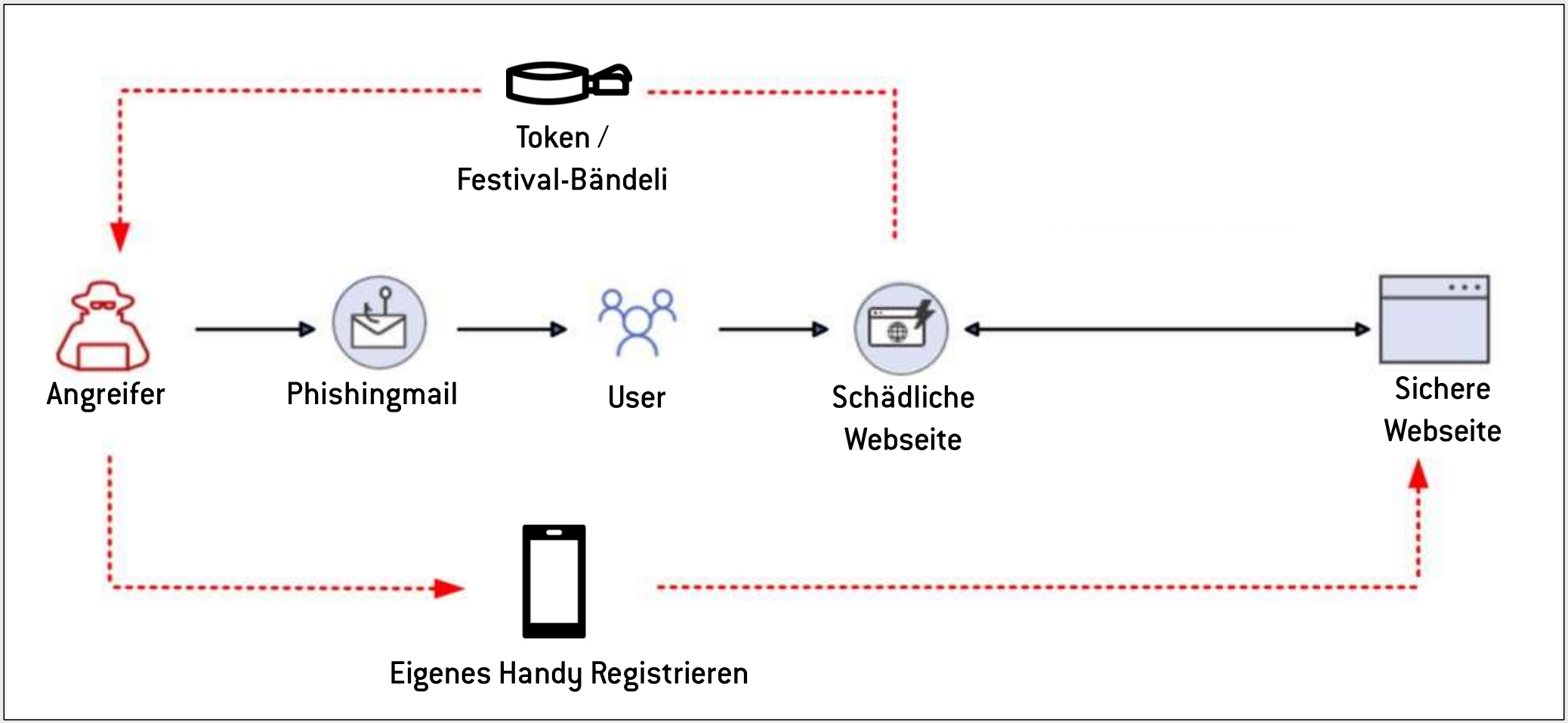
Schäden

- Reputation
- Rechnungen an unbekannte - 20K+

PRAXISBEISPIEL

WIE KANN EIN ACCOUNT ÜBERNOMMEN WERDEN?

first frame networkers



Richtangebot QA2025-355

An:

hat nun die folgende Datei sicher mit Ihnen unten geteilt.

Hier ist die folgende Datei, die sicher mit Ihnen unten geteilt hat.

Richtangebot QA2025-355

1 Minute, um dies zu lesen

Das funktioniert für jeden.

Öffnen

Microsoft

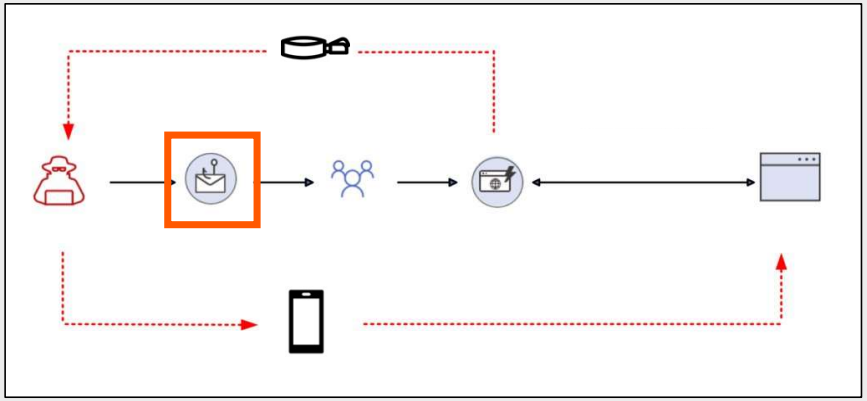
Privacy Statement

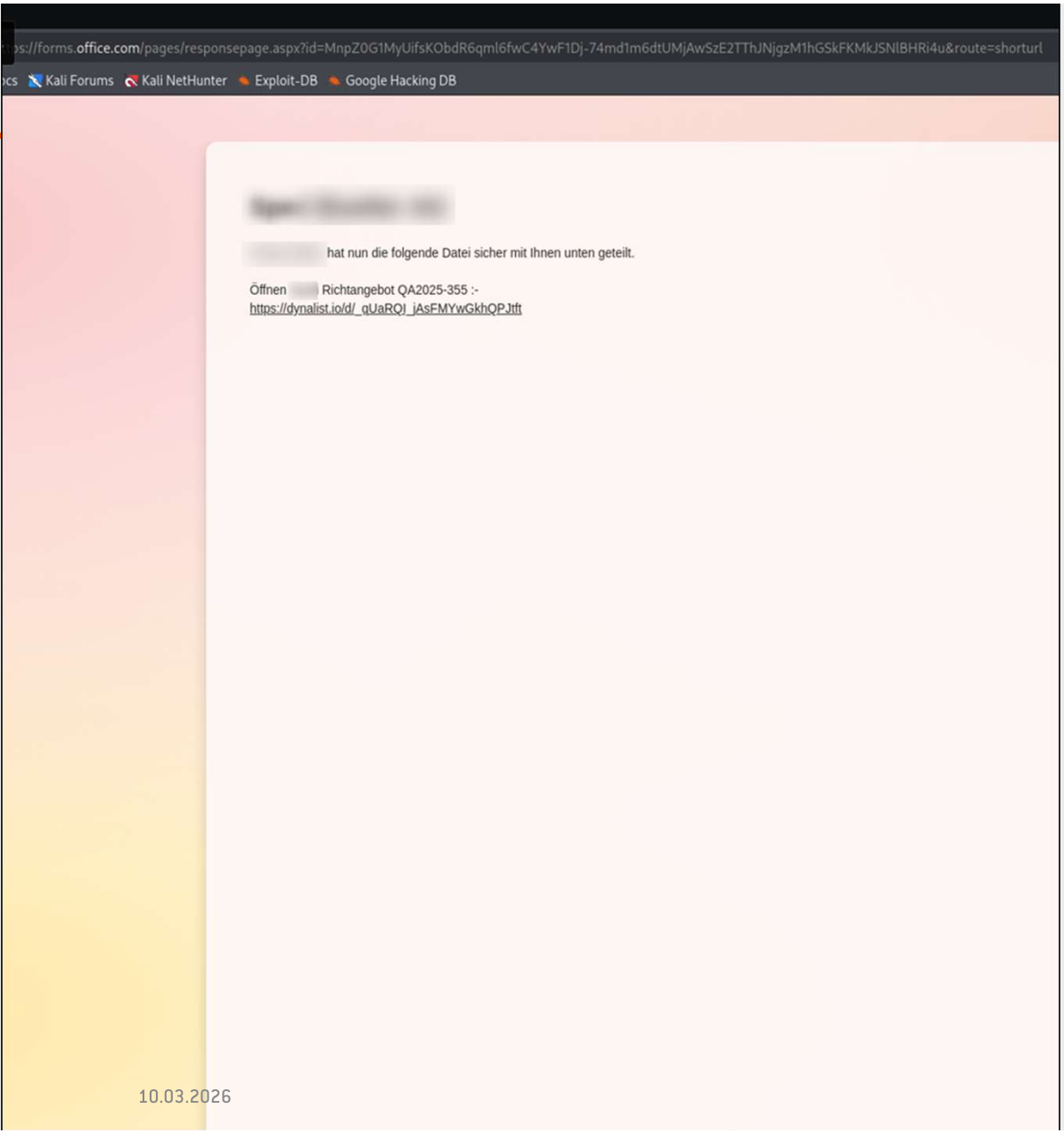
Freundliche Grüsse

first frame networkers

WIE FUNKTIONIERT EIN ACCOUNT-TAKEOVER-ANGRIFF?

PHISHING-MAIL

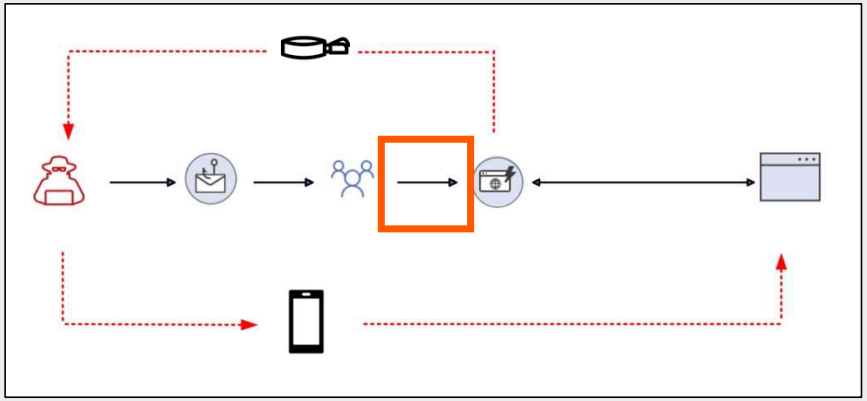


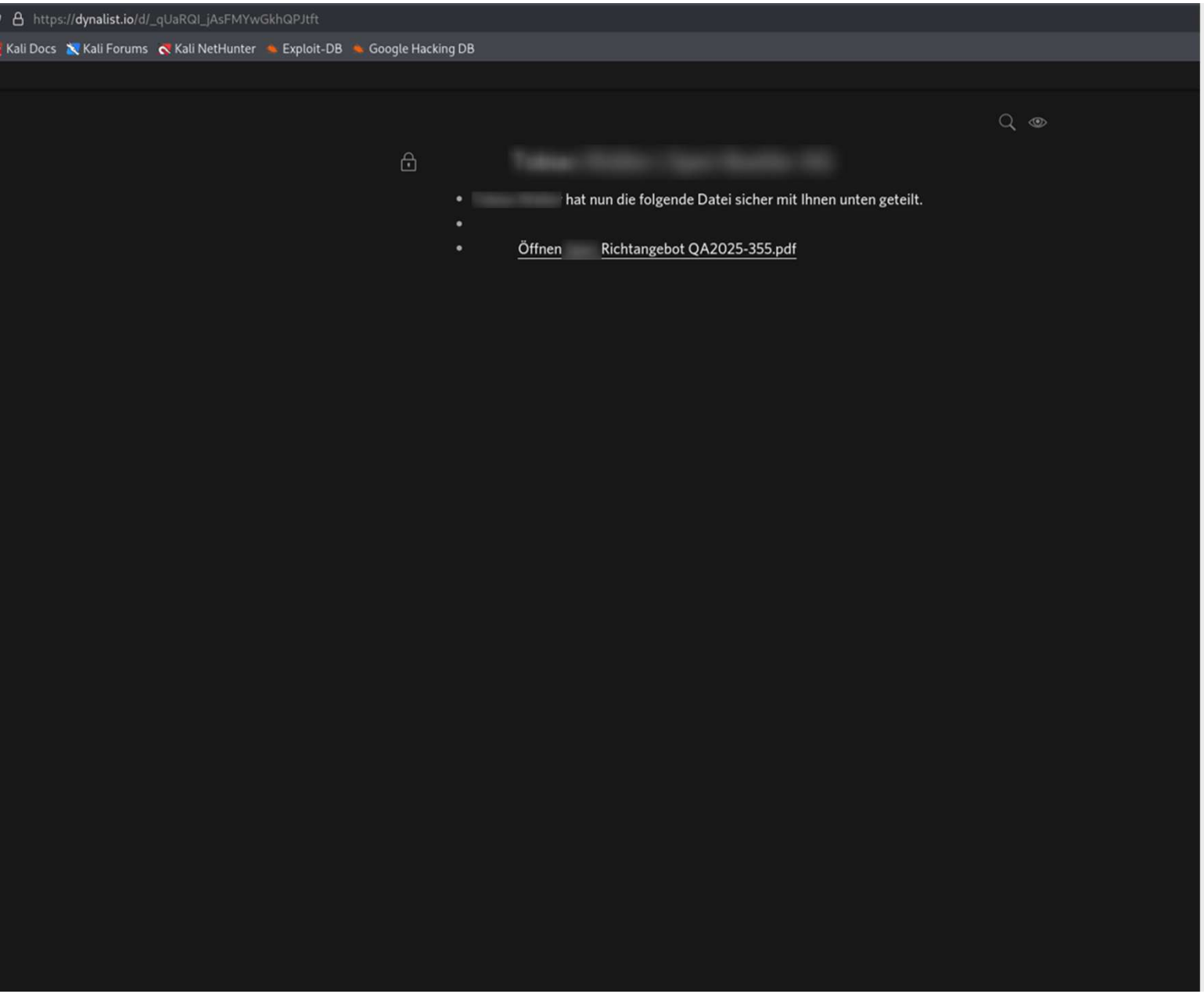


first frame networkers

WIE FUNKTIONIERT EIN ACCOUNT-TAKEOVER-ANGRIFF?

VERLINKUNG AUF MS FORMS





first frame networkers

WIE FUNKTIONIERT EIN ACCOUNT-TAKEOVER-ANGRIFF?

ÜBERGANG ZU LEGITIMEN EXTERNEN SERVICES, ALS ZWISCHENSCHRITT

https://kokoloko.blob.core.windows.net/kokoloko/

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB

https://kokoloko.blob.core.windows.net/kokoloko/

Connection security for kokoloko.blob.core.windows.net

You are securely connected to this site.

Verified by: Microsoft Corporation

More information

Microsoft

Sign in

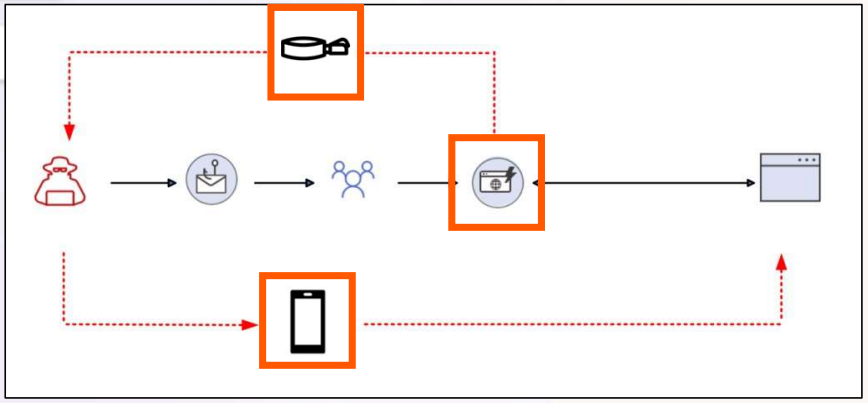
Email, phone, or Skype

No account? Create one!

Can't access your account?

Next

Sign-in options



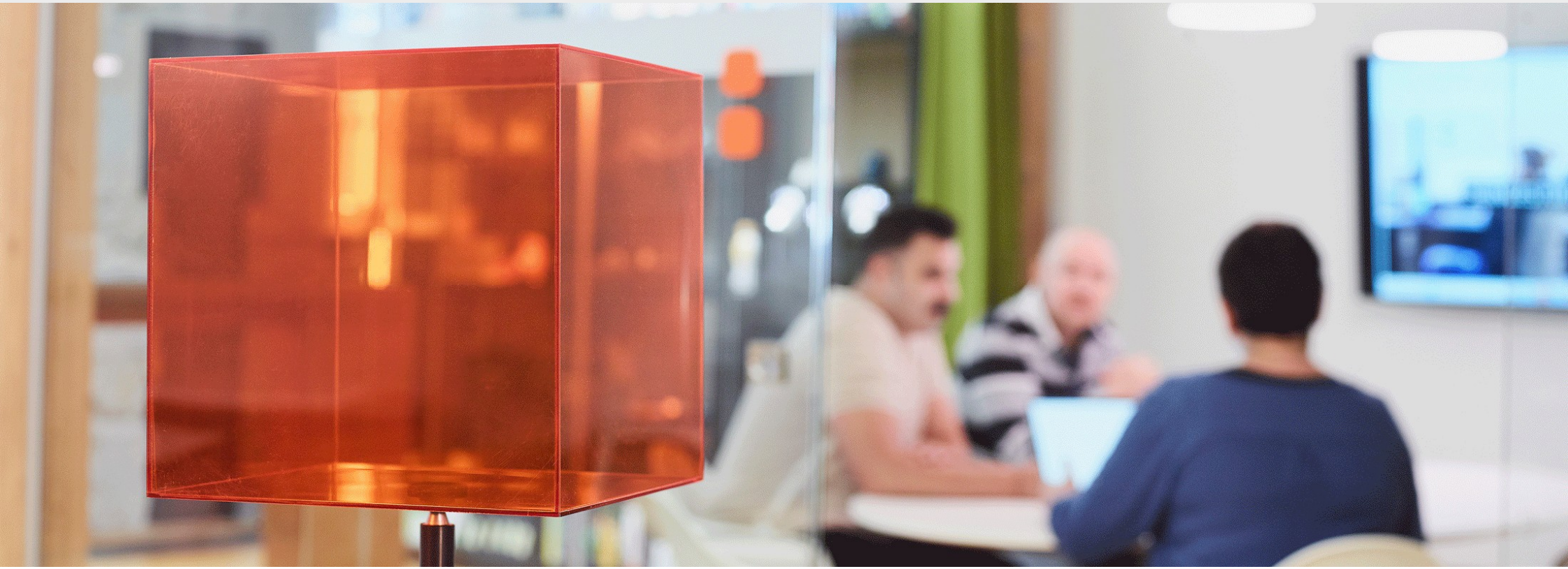
Terms of use Privac

WORAN ERKENNT MAN EINEN ACCOUNT TAKEOVER TECHNISCH?

first frame networkers

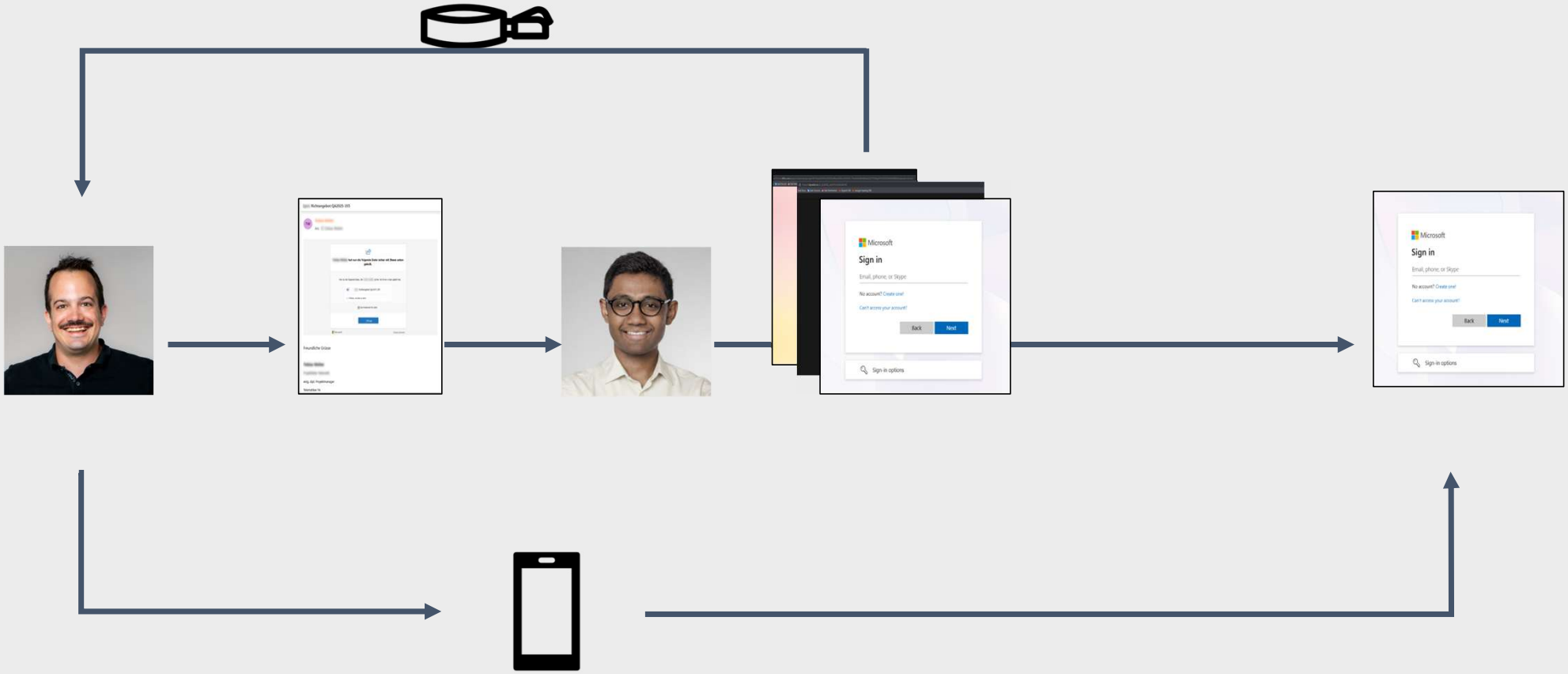
- Anmeldungen von ungewöhnlichen Orten
- Gefolgt von Registration neuer Mobilegeräte

GEGENMASSNAHMEN



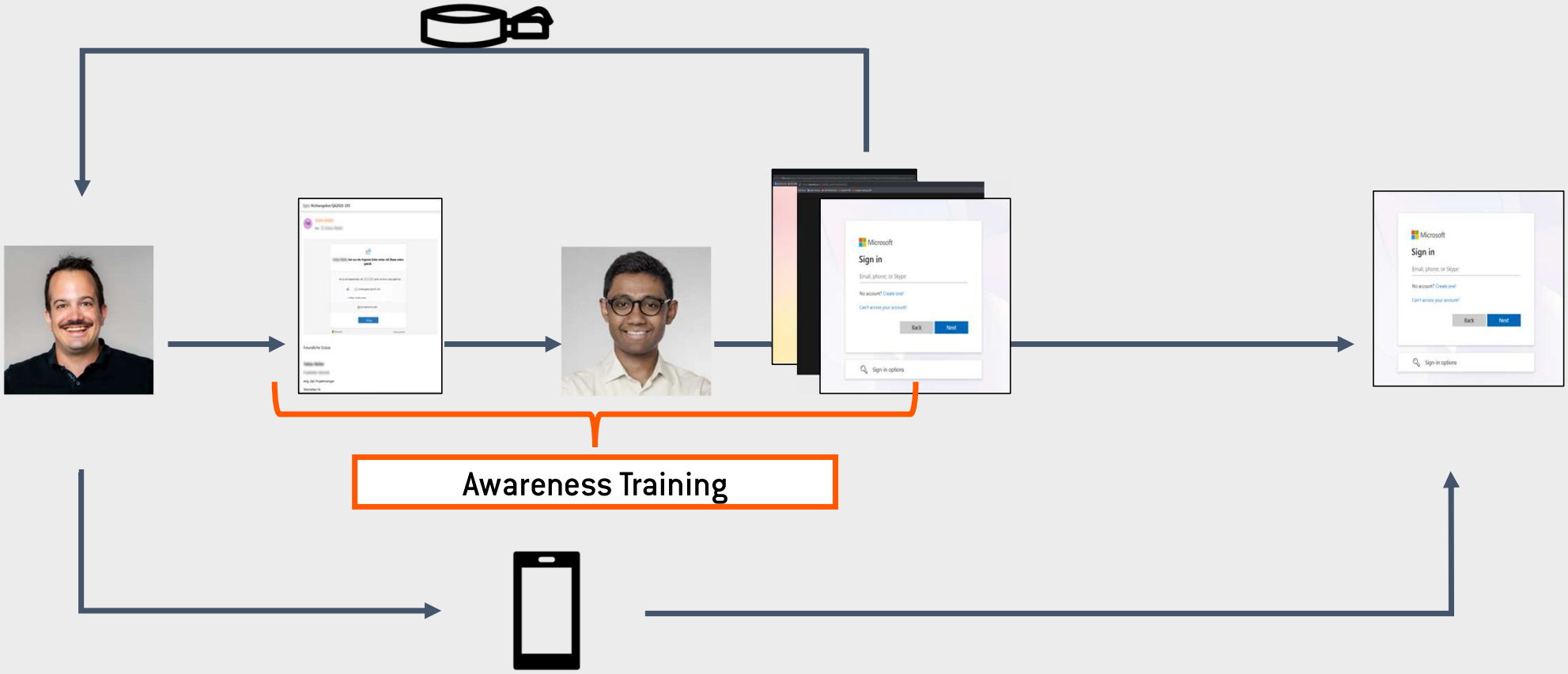
WELCHE MASSNAHMEN HELFEN DAGEGEN?

first frame networkers



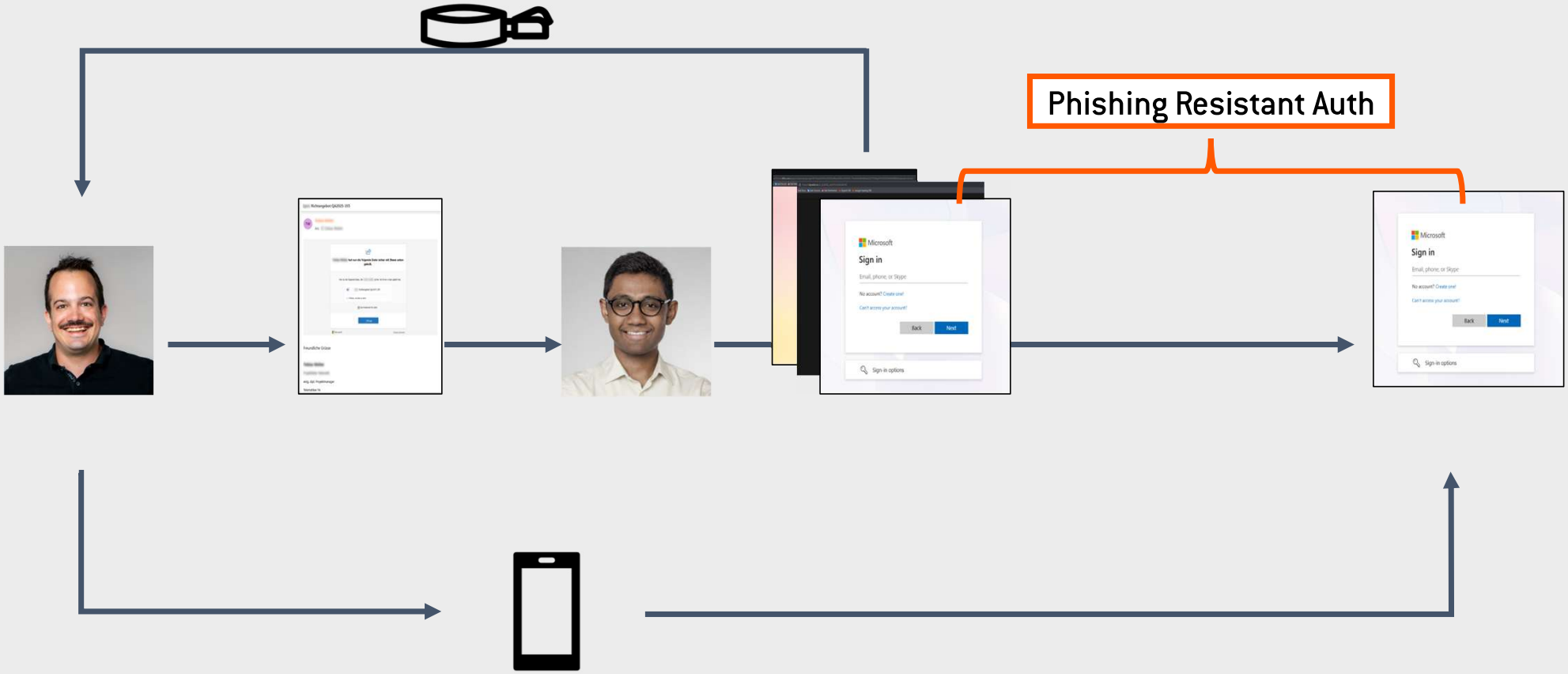
WELCHE MASSNAHMEN HELFEN DAGEGEN?

first frame networkers



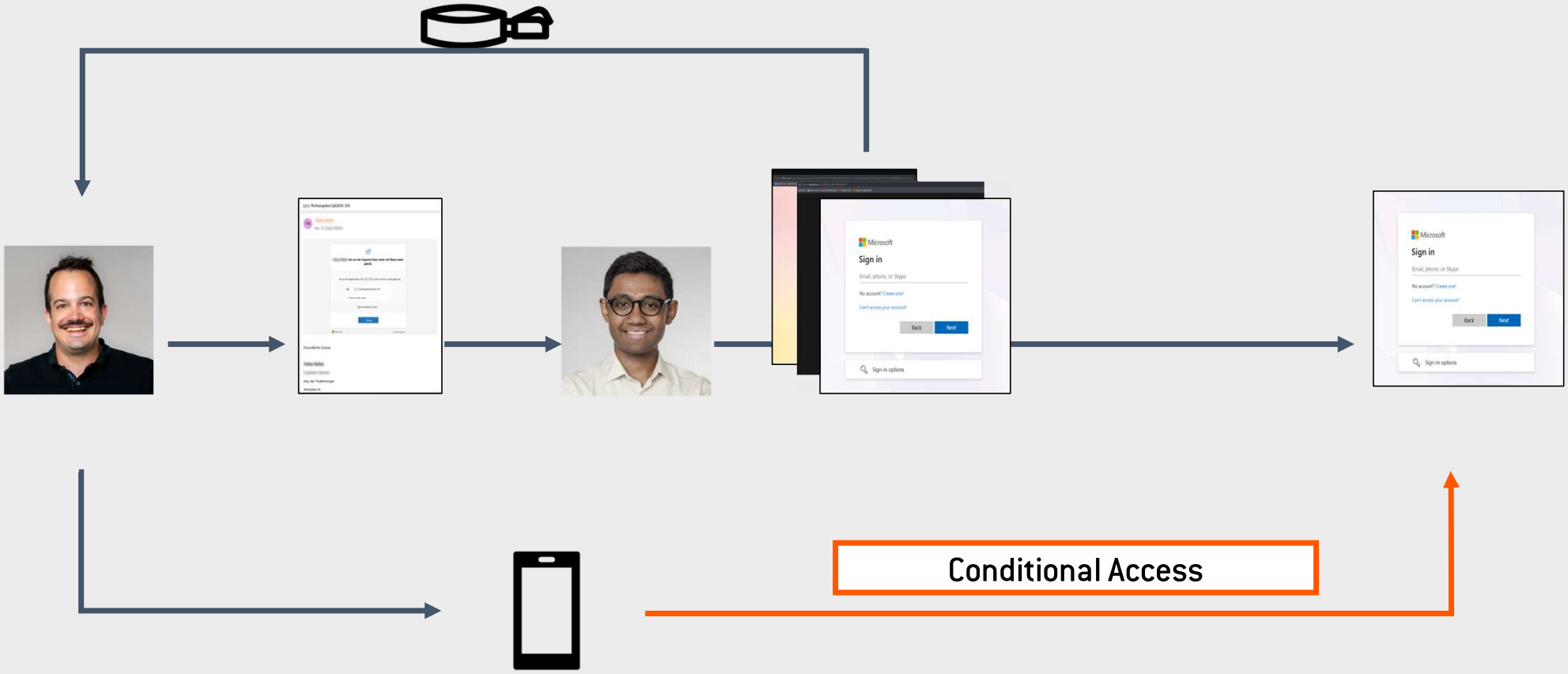
WELCHE MASSNAHMEN HELFEN DAGEGEN?

first frame networkers



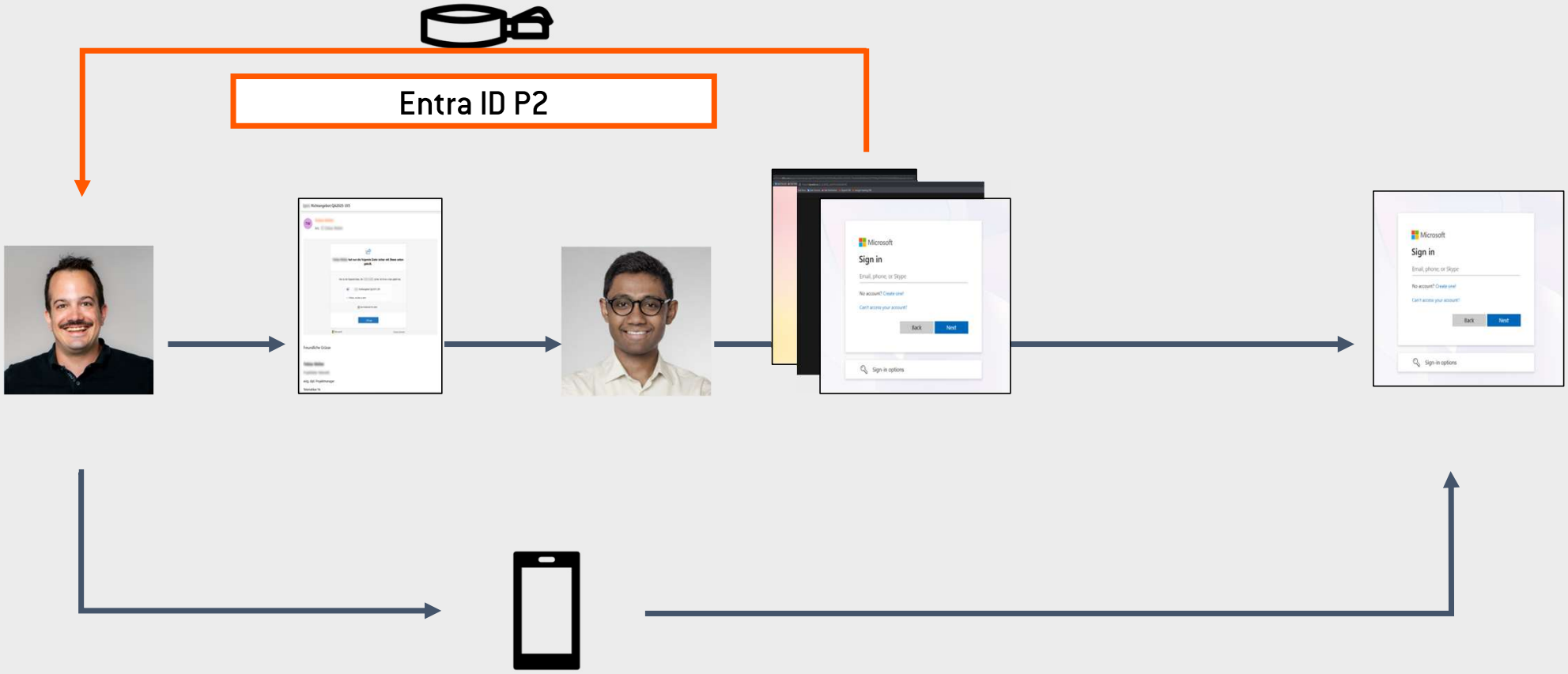
WELCHE MASSNAHMEN HELFEN DAGEGEN?

first frame networkers



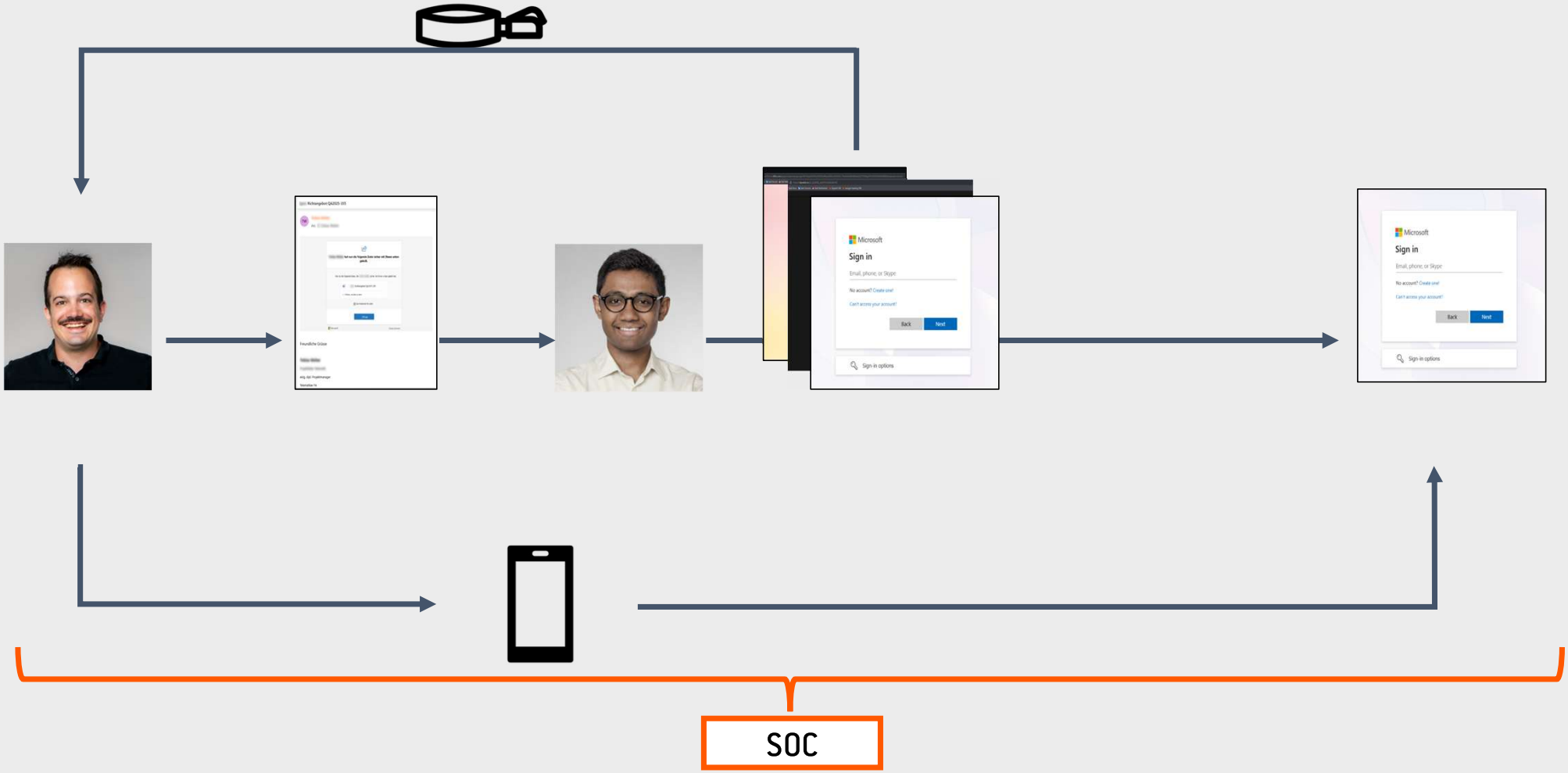
WELCHE MASSNAHMEN HELFEN DAGEGEN?

first frame networkers



WELCHE MASSNAHMEN HELFEN DAGEGEN?

first frame networkers

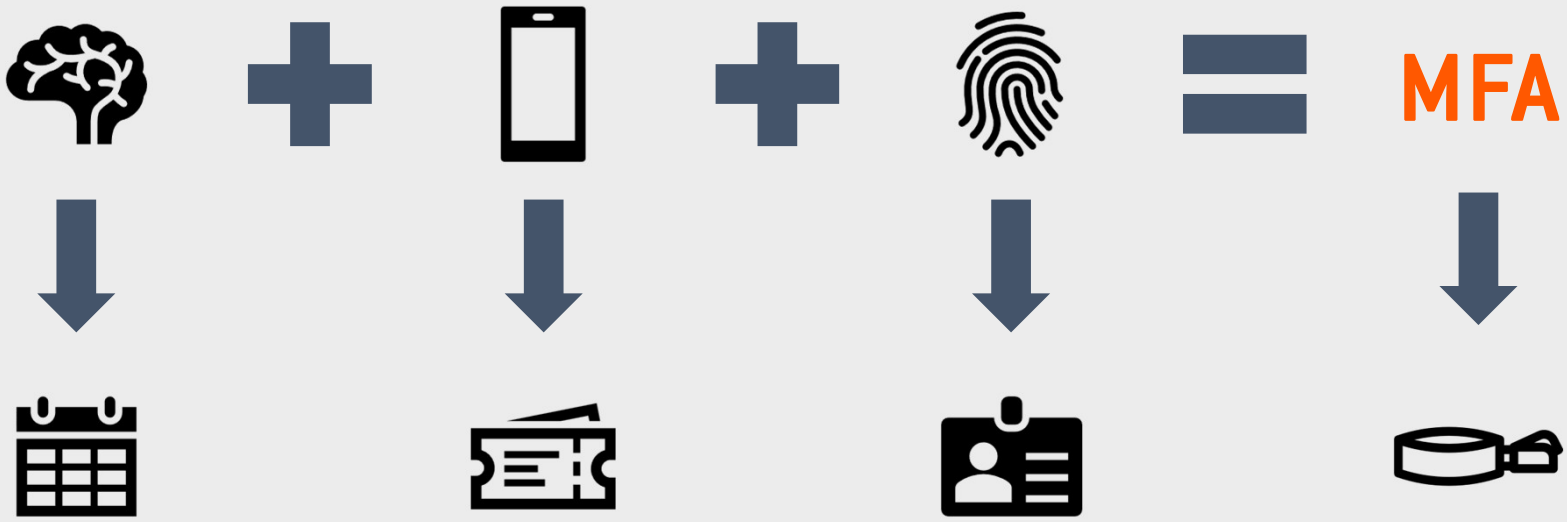


LESSONS LEARNED

WIESO KANN EIN ACCOUNT ÜBERNOMMEN WERDEN?

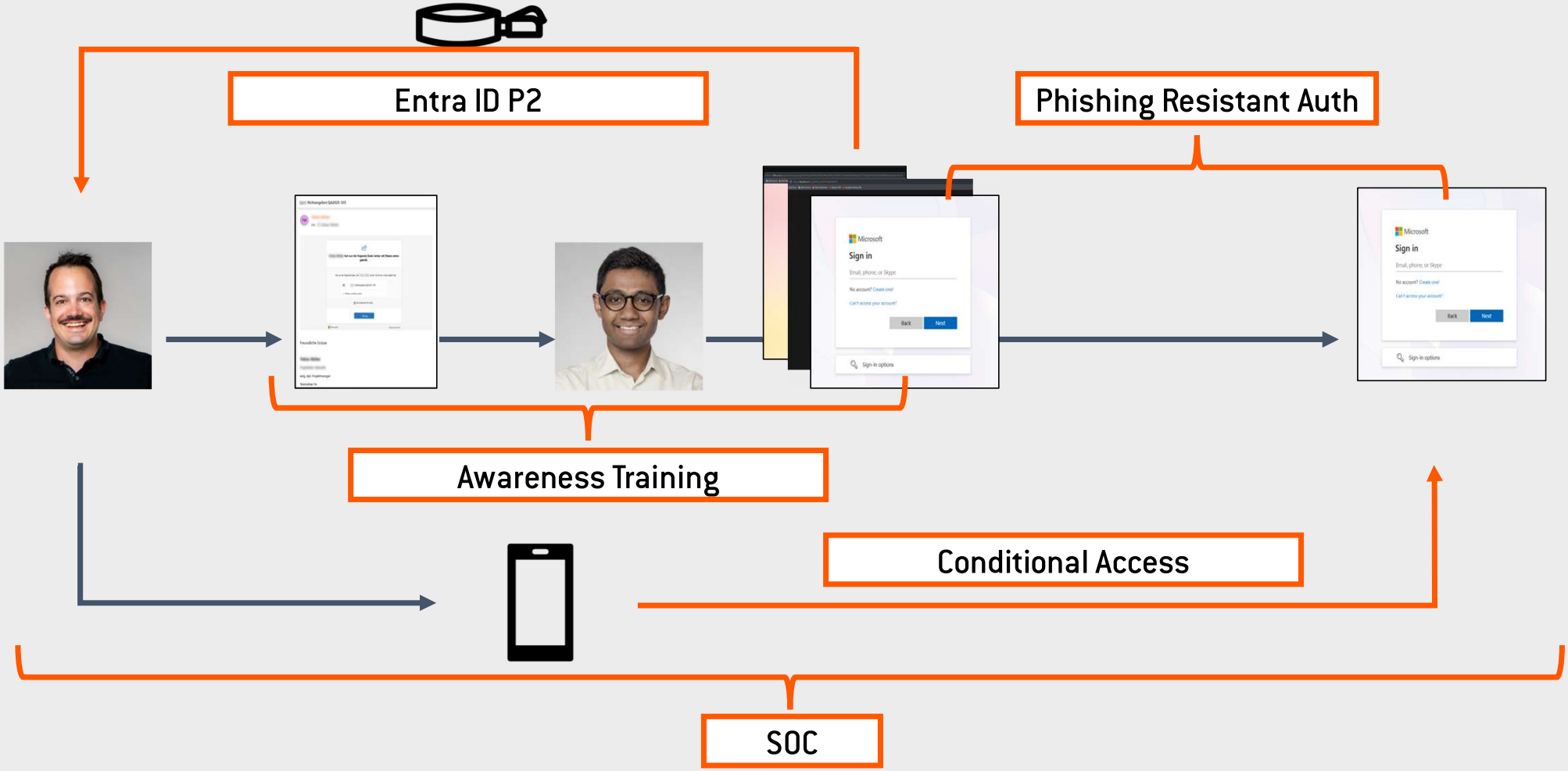
WIESO KANN EIN ACCOUNT ÜBERNOMMEN WERDEN?

first frame networkers



WELCHE MASSNAHMEN HELFEN DAGEGEN?

first frame networkers



WELCHE MASSNAHMEN HELFEN DAGEGEN?

first frame networkers

Awareness Training

- Gesundes Misstrauen gegenüber E-Mails
- Mehrfache Links anklicken -> komisch
- Wissen wo nachfragen
- Wissen wie melden

Phishing Resistant Auth

- Windows Hello for Business
- Passwordless Login mit Microsoft Authenticator
- Passkeys

WELCHE MASSNAHMEN HELFEN DAGEGEN?

first frame networkers

Conditional Access

- Einschränkung der MFA-Registrierung
- Token Protection

Entra ID P2

- Erkennt und blockiert impossible Travel
- Risikobewertung bei Login berücksichtigen
- Automatic Attack Disruption

WELCHE MASSNAHMEN HELFEN DAGEGEN?

first frame networkers

Technische Grundlagen

- Aktivierung von UAL
- Microsoft Sentinel + UEBA
- < 10.- CHF / Kunde & Monat

SOC

- Eigene Erkennungsregeln z.B. für ATO
- Reaktion auf Meldungen von Entra ID P2 und Defender
- Bereinigen von Überresten

WAS MACHE ICH ZUERST?

first frame networkers

1. Conditional Access & MFA einrichten
2. Aktivierung von UAL
3. Sentinel einrichten. < 10.- CHF pro Monat
4. SOC-Service beziehen
5. Security Awareness Training
6. Phishing Resistant Auth
7. Entra ID P2 Lizenzen

Q & A

first frame networkers

NEXT STEPS

first frame networkers

- Let's Talk!
  - Mit Ihrem Account Manager
  - Mit Philippe Hirzel philippe.hirzel@firstframe.net oder +41 41 768 08 60
  - Mit Arveenan Kamalakumaran: arveenan.kamalakumaran@firstframe.net oder +41 41 768 08 42
- Weitere Infos
  - Detaillierte Information Security Operations Center
  - Verschiedene Blog-Artikel zum Thema IT-Security

FEEDBACK-FORMULAR

first frame networkers

- Herzlichen Dank für Ihre Teilnahme am heutigen Webinar.
- Ihre Meinung ist uns sehr wichtig.
- Daher bitten wir Sie um eine Minute Ihrer wertvollen Zeit für die Feedbackumfrage.
- Unter allen ausgefüllten Fragebögen verlosen wir einen Bontique-Gutschein im Wert von CHF 75.—.
- Den Link finden Sie auch im Chat: https://forms.office.com/e/A8ZZ0sqqnR

Herzlichen Dank

first frame networkers